DOCUMENT RESUME

ED 324 012 IR 053 287

AUTHOR Trubow, George
TITLE Watching the Watchers: The Coordination of Federal Privacy Policy. Number 5.
INSTITUTION Benton Foundation, Washington, DC.
PUB DATE 89
NOTE 38p.; Project on Communications & Information Policy Options. For related reports, see IR 053 286-288 and IR 053 300.
AVAILABLE FROM Policy Options Project, Benton Foundation, 1776 K Street, NW, Washington, DC 20006 ($6.50 per single copy, $33.00 for boxed set of eight papers).
PUB TYPE Legal/Legislative/Regulatory Materials (090) -- Viewpoints (120)

EDRS PRICE MF01/PC02 Plus Postage.
DESCRIPTORS Access to Information; Agency Role; *Disclosure; Foreign Countries; Futures (of Society); *Information Dissemination; *Information Technology; Information Utilization; *Policy Formation; *Privacy; Program Descriptions; *Public Policy
IDENTIFIERS Information Policy; Office of Management and Budget; *Privacy Act 1974

ABSTRACT

In this policy briefing, the technological developments of recent years are linked to the erosion of individuals' informational privacy under the press of bureaucratic efficiency and the ever-growing needs of executive agencies for more information. It is noted that privacy protection within federal agencies may entail costs, and therefore, may be viewed as a constraint upon or impediment to the agency's mission. Discussion of these considerations points out that the Office of Management and Budget (OMB) is not likely to actively enforce privacy constraints because its purpose is to pursue cost reduction. It also indicates that data subjects themselves are largely unaware of potential privacy threats posed by information and technology practices, and that they have not organized into a constituency to focus on the issue. It is concluded that the Privacy Act of 1974 has not accomplished its mission, and that there is no existing device to adequately deal with privacy matters. It is proposed that Congress establish an independent agency charged with the responsibility of protecting federal information privacy. Related constitutional issues are raised, the general contours of an effective privacy protection mechanism are explored, and the makeup of data protection agencies in Canada, Federal Republic of Germany, France, Sweden, and the United Kingdom are briefly reviewed. (SD)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

* This document has been reproduced as received from the person or organization originating it.

* Minor changes have been made to improve reproduction quality.

* Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

ED324012

5

Watching the Watchers: The Coordination of Federal Privacy Policy

George Trubow

Benton Foundation
Project on Communications &
Information Policy Options

IR053287

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY

Karen Menichelli

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

The Benton Foundation

The Benton Foundation, based in Washington, D.C., is a private grantmaking foundation committed to improving the democratic process through increased public understanding and use of communications and information technologies. A legacy of Senator William Benton, the foundation supports projects in the fields of communications policy, public affairs and the media, and communications education.

Benton Foundation Project on Communications & Information Policy Options

In early 1988, the Benton Foundation commissioned a series of eight papers to explore future options for public policy in the communications and information arenas. Written by recognized authorities in their respective fields, the papers identify critical issues and options confronting policymakers at the federal level.

Through the publication of this series, the foundation seeks to stimulate public awareness and discussion of the communications and information issues that will affect our society in the coming decade. Two broad themes are addressed in the papers: the role of policy in the rapidly changing mass media marketplace; and the ethical, constitutional, and regulatory challenges that arise from the increasing use of computers in our society.

The views in this paper are those of the author(s), and do not necessarily represent those of the Benton Foundation, its directors, or its staff.

© 1989. Benton Foundation, Washington, D.C.

Watching the Watchers: The Coordination of Federal Privacy Policy

George Trubow

About the Author

George B. Trubow, A.B., J.D., University of Michigan, is Professor of Law, and Director, Center for Informatics Law, at the John Marshall Law School of Chicago, Illinois, where he teaches seminars on Information Law and Policy, and Privacy Law. Professor Trubow has served as deputy counsel to a subcommittee of the U.S. Senate Judiciary Committee, and as general counsel to the Committee on the Right to Privacy, Executive Office of the President, during the Ford Administration. He is Editor-in-Chief of the three-volume work, *Privacy Law and Practice*, published by Matthew Bender in 1987, and a member of the Council of the American Bar Association's Section on Science and Technology.

Executive Summary

Technological developments in the "information society" have eroded an individual's informational privacy under the press of bureaucratic efficiency and the insatiable hunger of federal agencies for more information. Early warnings about the encroaching technology and concerns over privacy and fair information practices led to the enactment of the Privacy Act of 1974. Though the OMB was given some limited responsibility in implementation of the Privacy Act, no plenary authority exists to monitor federal agency compliance with the Act or to make rules and regulations to carry out the purposes of the Act.

This paper proposes that Congress establish an independent agency charged with the responsibility to protect federal informational privacy.

Informational privacy protection is not an element of federal agency objectives. Agencies must accomplish their program missions as efficiently as possible. Privacy protection may entail administrative costs and may, therefore, be viewed as a constraint upon or impediment to the agency's mission. These same considerations are applicable to the Office of Management and Budget which is not likely to actively enforce privacy constraints because its purpose is to pursue cost reduction and promote mission-accomplishment by the executive agencies. Data subjects themselves are largely unaware of the kinds of privacy threats posed by technology and information practices, nor are they organized into a constituency to focus on the issue. As a result, the Privacy Act has not accomplished its mission, and there is no device in place to deal with the matter.

This paper proposes a comprehensive, plenary authority with adequate resources for research and study, rulemaking and rule interpretation, monitoring of agency practices, auditing of information systems, and adjudication of disputes regarding the collection,

use, maintenance, exchange, or disclosure of personal information. The structure of the agency should accommodate those program elements.

It is suggested that the board be composed of a chairman and four others appointed by the President and confirmed by the Senate; that no more than three members be from the same political party; that no board member serve as an officer, employee, or advisor of any other entity in the federal government or private sector; that board members be appointed for five years (except initially where staggered terms are established); and that no member may serve consecutive terms on the board. The chairman would be the chief executive officer of the board and would head its administrative office.

Each of the four other board members should head one of the following operational offices: administrative law judges, research and evaluation, auditing and enforcement, and general counsel. The board should issue rules and regulations and have power to conduct public hearings and to issue administrative subpoenas. Administrative law procedures should conform to the Administrative Practices Act. Decisions of the administrative law judges should be appealable to the federal district courts.

For purposes of comparison, the paper briefly reviews the makeup of data protection agencies in some other countries.

INTRODUCTION

There is in the United States today no effective mechanism for the development, coordination, or oversight of a comprehensive federal policy regarding personal privacy with respect to federal data banks. Faced with the realities of the contemporary "information society" and the computer revolution in information management processing, the individual's informational privacy is being rapidly eroded, sacrificed on behalf of bureaucratic efficiency and the endless hunger of federal agencies to develop and share larger and more refined data bases.

There have been plenty of early warnings concerning the jeopardy to privacy resulting from the new technology. In 1971, Arthur Miller sounded the alarm in *The Assault on Privacy*.[1] A. Westin and M. Baker, in 1972, clearly focused on the growing problem in their book, *Data Banks in a Free Society*.[2] A special task force of the U.S. Department of Health, Education, and Welfare, made the first in-depth government study of the problem and in 1973 issued its report, *Computers, Records, and the Rights of Citizens*, in which "principles of fair information practices" were first articulated;[3] they were also reflected in the Privacy Act of 1974.[4] In 1976, the Department of Justice issued guidelines regarding the security and privacy of criminal history records maintained in government data bases.[5]

In 1977, after a comprehensive three-year study, the Privacy Protection Study Commission issued its report, *Personal Privacy in an Information Society*.[6] The Commission made more than 160 recommendations for the protection of informational privacy, most of which have not been implemented because the Commission ceased to exist when its mission was completed and no other entity had responsibility to follow up its work. In 1981, the American Bar Association sponsored a National Symposium on Personal Privacy and Information Technology. The published report from the panel of distinguished participants[7] emphasized the privacy threats and

urged protective measures. A multitude of publications too numerous to catalogue here have echoed and re-echoed the previous warnings. Lisa Albinger, in the 1986 *Annual Survey of American Law*, succinctly summarized the nature of the problem:

> The right to privacy is integral to the American con ception of the proper balance of power between the people and their government. As long as a citizen abides by the laws, his personal affairs should remain free from excessive governmental scrutiny. In recent years, however, this balance has shifted. Federal agencies today maintain vast amounts of computer ized, easily accessible information on nearly every aspect of our lives. Unregulated access to this information threatens individual privacy interests....[8]

Personal privacy will continue to erode unless a positive and powerful program is put in place to preserve this precious human value. Accordingly, it is here proposed that Congress establish an independent agency charged with the responsibility to define and enforce a policy regarding federal informational privacy. It is not the purpose of this paper to prescribe that policy or to strike the balance of competing interests regarding access to personal information in government files. That is precisely the complex and continuing responsibility of the agency to be described herein. The paper will, however, suggest some approaches to that task. Additionally, another paper in this series (see *A Federal Right of Information Privacy*, by Jerry Berman and Janlori Goldman) addresses revisions of the Privacy Act necessary to clarify and strengthen the federal policies for privacy protection. An improved Privacy Act that sets out federal policies could be administered by the agency outlined in this paper.

The paper is organized as follows: after a few definitions to clarify the author's perspective and terminology, there is a brief description of how the new computer technology has altered information management in a way that threatens to destroy informational privacy. Next there is a discussion of why the measures pursued

thus far have been inadequate to deal with incursions on informational privacy. Several examples are offered to illustrate the piecemeal, conflicting, and incomplete steps that have been taken by the federal government to protect informational privacy, describing the fragmentation of responsibility for information policy among a variety of federal executive and legislative entities. Further, the judiciary is hampered in making sound case-by-case determinations because there is no adequate framework of federal policy for delineating "privacy." After a discussion of constitutional constraints arising from the separation of governmental powers, the paper sets forth the general contours of an independent privacy protection board to oversee federal data banks. The paper then identifies the program elements needed to adequately accomplish the tasks of refining and monitoring a federal informational privacy policy, as well as dealing with the resolution of disputes among agencies or between agencies and data subjects. Finally, there is a brief comparative description of some data protection commissions in other countries.

A NOTE ON THE PAPER'S FEDERAL SCOPE

The subject of this paper is a mechanism to implement policy regarding privacy protection in federal information systems. It should be clearly understood, however, that in this time of technological advances that encourage information exchanges, it is not sufficient to address merely the federal role in information processing. The federal government receives great quantities of personal information from state and local government and from the private sector. The Privacy Act, the principal statute regarding the subject of this paper, does not address the *acquisition* of information by federal agencies; it is primarily concerned with what the agencies do with personal information once they have it. Thus, individual privacy may be compromised by the disclosure of information by the private sector to federal agencies, as well as by the exchange of information among state agencies and the private sector — none of which is within the purview of the Privacy Act.

State governments and the private sector hold the vast bulk of personal information concerning the residents of this country. Informational privacy protection will be woefully inadequate if the states and private sector are not encouraged or required to observe essentially the same protocols deemed applicable to the federal government.

When the Privacy Act of 1974 was under consideration, the Administration opposed bringing state government or the private sector within the Act, or establishing a single agency with plenary oversight of informational privacy. The reasons were that (1) information management practices, especially with respect to privacy interests, were extremely poor and it was thought to be a better idea to get the federal house in order before establishing guidelines for private sector information management, and (2) at that early stage it seemed unwise to establish an "information tsar" since experience with privacy protection was lacking.

The troublesome question of "Who watches the watchers?" discouraged the centralization of information power. Though Privacy Act sponsors in Congress favored some private sector regulation and an oversight agency, as a compromise the Privacy Protection Study Commission was established for a two-year period to study, among other things, the matter of private sector information protocols. Also, some limited oversight authority for Privacy Act implementation was given to OMB. However, OMB was not intended to have a pervasive role in setting, monitoring, or enforcing informational privacy protection by the executive agencies that gather and use personal information.

Almost 15 years have elapsed since the Privacy Act was passed. The recommendations of the Privacy Protection Study Commission have been largely unheeded by the private sector; as pressure by the federal government for privacy regulation has abated, so has the interest of the private sector in pursuing the protection of informational privacy. Segments of the insurance industry, for instance, implemented privacy protection policies soon after the issuance of the Commission report; there is no evidence that other personal

information-oriented industries of the private sector have voluntarily done likewise.[9]

It may be that good federal practices, established and enforced, will themselves be a guide for the voluntary adoption by state government and the private sector of similar protocols. Certainly, we must begin somewhere, and an exemplary federal program may provide a model to be emulated. The author has little faith that such might occur; experience subsequent to the Privacy Act suggests otherwise. Our belief is that a firm national policy will be necessary for adequate privacy protection to be implemented and respected by *all* record keepers. Though such a program is not the task of this paper, the author does not want readers to infer that regulation of federal agencies alone is enough simply because that is the focus of this paper.

DEFINITIONS

At the outset, some definitions will help to clarify terms that may be subject to misunderstanding.

The word "privacy" is much in vogue today, and is used to describe a variety of personal interests.[10] There are four separate kinds of "privacy" in our common law of torts. These deal with intrusions into private places, unpermitted use of someone's name for commercial purposes, the false and objectionable portrayal of one's lifestyle or personal characteristics, or the general publication of private information. None of them addresses directly the problems that arise out of the management of personal information in government data banks.[11] There are also aspects of personal dignity that comprise "privacy" as protected by the U.S. Constitution, such as procreation or the integrity of the human body; these also are not within the scope of concerns here.[12] Instead, we focus on what we call "informational privacy," which is the interest in the collection, maintenance, use, and dissemination of personal information.[13]

Personal information is any information that describes a natural person, and thus is defined by the reference of information and not by its content. Thus, so long as information refers to an identifiable

individual — whether that reference is made by a person's name, or a number, or some other identifying characteristic — then it is personal information.

The *data subject* is the one to whom personal information refers; a *record* or *file* is a collection of personal information, and *a data element* is one "piece" of information in a file; the *"identifier"* is the data element that connects information with a particular data subject.

The *record holder* is the entity that maintains the data base or controls access to it; a *data base* is simply a collection of stored information, whether in manual or automated files, that may be systematically accessed. *"Access"* is to gain entry to or read a file or data element, and *dissemination* means the communication of information to a third party — someone other than the data subject or an authorized agent of the record holder.

Security refers to the technology or procedures that safeguard information, protecting it from unauthorized access, alteration, or loss. Information is *confidential* if access to it is limited to specified entities or purposes; information is *secret* if only the record holder and a chosen few know that the information itself exists. (Criminal records are confidential — everyone knows that such files are kept, though access to them is controlled. On the other hand, there was always popular speculation about whether J. Edgar Hoover had his own secret files on political notables.) A *public record* is open to anyone.[14]

COMPUTER TECHNOLOGY AND INFORMATION MANAGEMENT

Modern technology makes it possible to collect, store, manipulate, and disseminate information at the speed of light and in quantity and quality never before imagined. The advent of miniaturization makes possible the micro or "personal" computer, so that for a few hundred dollars virtually anyone can own a sophisticated information processor. Modems allow computer users to connect their machines with data bases around the world, so that

with appropriate identifiers one has a virtual central data base composed of information gleaned from distributed data bases in automated systems everywhere. The contents of the Library of Congress can be stored on a few discs, so that constraints of space regarding information storage have been all but eliminated.

Because it is relatively easy and cheap to collect and store data, the limitations of cost that used to be a natural disincentive to the collection and storage of information have been markedly reduced. In 1981, based on data on using IBM mainframe systems, the United States Congress Office of Technology Assessment found that the cost of performing 100,000 calculations on a computer system had dropped from $1.26 in 1952, to $0.0025 in 1980.[15] Though there has been no occasion for a more recent cost analysis, it is common knowledge that since 1980 the cost of computer systems has continued to drop in relation to the enormous increases in data processing capability.[16]

The three billion files of personal information maintained by the federal government[17] were but a small privacy threat when that information was manually stored and buried somewhere in stacks of paper archives. Today, as that information is converted to automated files,[18] it is instantly available. What had been a theoretical threat to informational privacy has become a real one.[19] The various automated data bases maintained by federal agencies can be linked together electronically so that, as the Office of Technology Assessment concluded in a recent report, in reality a virtually centralized data base on United States citizens is now available.[20] To make matters worse, the Tax Reform Act of 1986 authorized the use of the Social Security number (SSN) for a wider range of personal files, and requires everyone over the age of five to have a SSN.[21] Though directed at improving the efficiency and effectiveness of the government's tax programs, the law served to make the SSN an even more convenient and pervasive tool for locating, retrieving, and linking personal information in government files.

Indeed, Congress recognized the inadequacies of the Privacy Act with respect to regulating the linking and cross-matching of federal computer files by enacting the Computer Matching and Privacy Protection Act of 1988.[22] The Act requires the development of policies to avoid the kinds of privacy invasions as have been discussed above, though that Act itself could be more effective were it to be administered by such an agency as described later in this paper.

FRAGMENTED FEDERAL PROTECTION

The "Watergate era" focused public attention on the illegitimate use of personal information that had been collected in federal files for legitimate purposes.[23] That attention led to the passage of the Privacy Act of 1974, which was designed to give the data subject a measure of control over personal information in federal files.[24] The principal provisions of the Privacy Act are designed to give notice to the public of federal information systems that store personal data, give a data subject the right to review and challenge the accuracy of files about him or her, and restrict the exchange or disclosure of personal information. As is discussed later, the Act has fallen short of expectations, but more importantly, it is not enforced by any agency with the power or responsibility to protect informational privacy.

Prior to the Privacy Act, only the Freedom of Information Act,[25] enacted in 1966, gave the individual any significant rights regarding information in federal files, and that was for the purpose of providing access to information about government.

The presumption of the Privacy Act is that personal information is confidential and thus closed to third parties, with specific exceptions. The Freedom of Information Act, on the other hand, begins with the presumption that government records are open to the public, *except* for specified reasons.[26] Thus, when personal information is in a federal record, the basic differences between the Privacy Act and Freedom of Information Act create conflicts regarding informational privacy protection.[27] Resolution of such conflicts is difficult if not impossible because the Department of Justice has oversight over the FOIA while OMB is responsible, to a limited

extent, for the Privacy Act; there is little evidence of coordination between OMB and DOJ regarding the intersection of these two Acts in the privacy dimension.

The decisions pursuant either to Privacy Act or FOIA requests rest initially with the various federal agencies to which inquiries are addressed. The factors on which decisions are based as to the privacy interest of the data subject and the public "need to know" vary widely depending upon the nature of the information sought and the purpose for which the government maintains it. A multiplicity of agencies have developed a multiplicity of standards that have been applied in striking the balance between confidentiality and disclosure. In such circumstances, coordination through oversight is crucial for a consistent, even-handed policy.

While Congress did not establish an agency to coordinate implementation of the Privacy Act, it gave some limited responsibility to OMB, mainly to develop some general guidelines for the agencies and to report periodically to Congress on agency activity pursuant to the Act. There has been ample criticism of the inadequacies of privacy protection through OMB oversight. For instance, from an OTA report:

> All of the studies evaluating the implementation and effectiveness of the Privacy Act cite its major weaknesses to be its reliance on individual initiative; the ambiguity of some of the act's requirements; the casual manner in which OMB has implemented and enforced the act; and OMB guidelines issued subsequent to the act that seem to contradict the purpose of the act.[28]

And, from a report of the General Accounting Office:

> The pervasiveness of such shortcomings leads us to conclude that Privacy Act operations need a cohesive, articulated program aimed at assuring that such activities are conducted in full compliance with OMB guidance and the act's provisions. In our opinion, without more active involvement and monitoring by both OMB and

> agencies, there will be less than full assurance that Privacy Act functions are carried out in a manner that protects the privacy rights of individuals and balances these rights with the information needs of federal agencies.[29]

It should not be a surprise that informational privacy is not vigorously pursued by OMB or other federal agencies. The reason is simple: the protection of individual privacy is *not* a rational element of federal agency objectives. The agencies are supposed to accomplish their own program missions (which do not include privacy protection) as efficiently as possible, so their natural tendency will be to use the information in their records in ways that suit their purposes, and the privacy interests of the data subject will probably be irrelevant.

Further, the protection of informational privacy may be antithetical to an agency's budget concerns, because the protection of privacy will entail administrative costs in technology and procedures to assure that the confidentiality of information is real and effective. Thus, privacy protection can be viewed as a constraint upon or impediment to agency mission accomplishment and information processing cost-containment.

These same considerations of the executive department operating agencies apply also to OMB. The "fox in the chicken coop" is certainly not likely to actively enforce privacy constraints upon its sister agencies because the OMB pursues cost reduction and promotes effective mission-accomplishment by executive agencies. It is, therefore, understandable that OMB has been roundly criticized for ineffective privacy protection policy, as has been previously cited. A parallel observation has been made about the DOJ role in FOIA oversight:

> [T]he Department of Justice is frequently a participant in FOIA disputes. In some attenuated sense, they are a participant in every FOIA dispute. Even if it is not a Department of Justice element involved, then the Department of Justice has probably promulgated policies that have bearing on how the agency has handled that

> problem or rendered advice or may be in a position of being about to litigate the case. That makes the Department of Justice an interested party, and I think if you put an ombudsman next door to an interested party as part of the same organizational structures, you don't get an independent, the kind of independent authority that you need to play an ombudsman role effectively.[30]

Accordingly, suggestions merely to strengthen the OMB role will miss the mark. The result would be to make OMB more effective in pursuing administrative policy at the expense of informational privacy.

Another reason for the lack of privacy protection is that data subjects themselves are largely unaware of the kinds of privacy threats posed by technology and information practices, and they are not organized into a constituency to focus on this issue or to bring pressure on the government. Information is not an end in itself; rather, it is the means to other ends — it is the grist for decision-making. As might be expected, people ordinarily focus on the decision to be made, and not on the practices by which information for the decision has been secured. With the exception of a few public interest groups such as the American Bar Association or American Civil Liberties Union, no major constituency is pressing for increased informational privacy. This specific point, incidentally, was noted in the ABA Symposium report mentioned earlier: "The individual's informational privacy is relatively unprotected and will remain so unless an effective constituency is developed....Some long-term mechanisms...must be established to...develop informational privacy policy."[31] To put it another way, no one is watching the watchers!

It seems clear, then, that privacy has suffered, and will continue to do so until an independent federal agency is established that is concerned with informational privacy as its principal mission. Such a suggestion is not a novel idea; there have been other similar suggestions proposed in the recent past.[32] Without seeking to belabor the point, we cite Lisa Albinger once more:

A possible administrative solution to the problem of protecting privacy would be the creation of an independent public agency to oversee the government's collection and use of information. The original Senate version of the Privacy Act proposed the establishment of a permanent Privacy Protection Board. However, the final compromise legislation instead created the Privacy Protection Study Commission, whose term has since expired.

Attacking the problem of data accumulation by creating yet another agency with voluminous records may seem paradoxical. However, it would be far easier for the public to address problems to one independent agency than to locate the department within a given agency that deals with privacy concerns. At present the burden of regulating information flow is on the public and the agencies. The agencies have an inherent conflict of interest; they need more information to perform their duties effectively and will inevitably seek to justify additional information collecting on efficiency grounds. Individual citizens simply do not have the resources to police government agencies. A "watch-dog" agency to oversee privacy concerns would be in a better position to strike the necessary balance between the government's need for information and the citizen's need for privacy.[33]

CONSTITUTIONALITY OF AN INDEPENDENT AGENCY

Congress has established literally dozens of independent agencies, and the constitutional legality of such a device is beyond question. It may be useful, nevertheless, to describe briefly the necessary constitutional ingredients that will be reflected in the proposal that follows.

Generally, Congress may delegate regulatory powers to administrative agencies so long as Congress provides a program outline — "intelligible principle." In *Wayman v. Southard*, 23 U.S. (10

Wheat.) 1 (1825), Chief Justice Marshall, writing for the Court, acknowledged that Congress could not properly supervise all the day-to-day details of national government. The Court held that Congress may delegate powers to agencies so long as Congress established "the general outline of the regulatory program" and allowed the agency to fill in the details. The Privacy Act, as amended, provides the necessary regulatory program outline. That Act will need amending in contemplation of the new administrative agency, a need that can be addressed in the authorizing legislation.

So long as certain conditions are satisfied, Congress may, pursuant to Article I, vest administrative agencies with powers to decide certain cases and controversies. These administrative courts have been held constitutional because the legislature created them to make factual and legal determinations concerning "public rights." Subsequently, these tribunals have been upheld even where private rights are adjudicated, so long as the parties have a right to appeal to an Article III court. The proposal hereafter is consistent with these principles.

GENERAL CONTOURS OF AN EFFECTIVE PRIVACY PROTECTION MECHANISM

For there to be a truly effective agency for informational privacy protection, it must have comprehensive, plenary authority and adequate resources for research and evaluation, rulemaking and rule interpretation, monitoring agency practices and auditing information systems, enforcement of privacy policy, and adjudication of disputes regarding the collection, use, maintenance, exchange, or disclosure of personal information. It is beyond the scope of this paper to present a detailed draft of authorizing legislation. It is enough to describe the programs and functional authority of such an agency. Hereafter, the mechanism to be proposed will be referred to simply as "the Board."

Congress has acknowledged a need for better privacy oversight through passage of the Computer Matching Act of 1988, mentioned above. That legislation would authorize data protection boards

within executive agencies that operate computer file matches. Such boards, however, would suffer still from inherent conflicts of interest and the need for coordination and uniformity that can only be met by a single oversight authority.

Given the variety of independent agencies now in existence, there are many models for configuring such an agency. The particulars of structure depend upon the nature of the program elements appropriate to the Board's objectives and functions.

PROGRAM ELEMENTS

Research and Evaluation

In light of the dizzying speed of new information and communications technology development and the continuing demands for access to personal information, it is imperative that the Board keep abreast of these matters and consider their impact on government, society, and individuals. Because new technology affects the collection, storage, and retrieval of information, the Board should remain current regarding information processing techniques. Consultation with the various agencies, and with information users and public interest groups can help the Board to anticipate the privacy concerns attendant upon requests for the collection of new information or new uses for available information. The regulations issued by an informed Board can ameliorate negative impact on informational privacy while not impeding the reasonable development or application of new technology or procedures. Periodic studies of the impact of personal information disclosures and exchange by federal agencies and surveys of public attitudes regarding governmental sensitivity to informational privacy can help the Board assess the value and tenor of federal information practices.

Rulemaking and Policy Interpretation

The general framework for the government's information policy and privacy protection will be prescribed by the Congress in the Privacy Act and elsewhere, but the Board's rulemaking and interpretation for the implementation of that policy will be chief among its functions. The Board must be empowered to make rules governing the procedures by which agencies will implement the Privacy Act, and to determine whether federal information management practices satisfy the policy objectives of the Act. No agency should collect personal information, nor establish new personal information systems, without Board approval.

The needs and exigencies pertinent to particular programs and information systems require sufficient flexibility in regulation so as not to unreasonably encumber the bureaucracy nor discourage implementation of cost-effective practices. At the same time, the discontinuity and confusion that arises from the establishment of variant information policies and practices by a multitude of agencies can be avoided by the Board's unitary oversight. Clear and uniform policies reduce uncertainty and the need for litigation; lawsuits result when individuals are without adequate guidance regarding how a disagreement should be resolved.

Enforcement

The enforcement of privacy policy will be a critical necessity for the successful protection of informational privacy. The Board must be empowered to issue advisory opinions to agencies for the purpose of suggesting procedures or practices that satisfy privacy requirements. The Board must also be authorized to issue specific orders directing agency compliance with privacy policy or requiring that certain practices be altered or terminated. Agencies should comply with Board directives promptly or within such time as the Board may allow; failure by an agency to comply with Board rules or orders should be reported by the Board to the President and to the appropriate oversight committees of the House and Senate.

Monitoring and Auditing

Responsible oversight requires the ongoing monitoring of agency compliance with the policies established by the Congress. It is not sufficient for the Board merely to await questions from agencies or complaints from citizens; instead, it should routinely inspect for sufficiency the systems used and procedures promulgated by the agencies pursuant to Board rules and guidelines, and should disapprove and require correction of those systems or practices deemed inadequate. The Board should review periodic statistical reports from the agencies (which they are already supposed to provide to OMB pursuant to the current provisions of the Privacy Act) to assess agency workloads, timeliness of response, and patterns of personal information disclosure or exchange.

This function need not engender unreasonably burdensome agency reports or red tape; new information technology can be utilized to monitor the flow of personal information transactions. Here, especially, it is necessary to avoid perceiving this activity from the perspective of paper-based information processing, but instead to realize the ease and economy which the technology itself can provide. Also, the availability of consultation with the Board and its staff can help executive department officials make speedier and sounder decisions for information management practices that are consistent with a respect for privacy.

Auditing involves the periodic inspection of system hardware, software, and operations, to assure that the integrity, confidentiality, and security of information is maintained. The Board's auditors should periodically examine in detail an agency's process for treating personal information transactions from beginning to end, sampling requests from or disclosures to agencies, data subjects, or third parties. The security programs for personal information systems should be challenged, and internal agency procedures to protect information should be tested. As noted earlier, new technology can help to accomplish this goal as a by-product of the functioning of the information systems themselves. Further, a uniform government-wide observance of appropriate system security levels may cut costs by eliminating unreasonably expensive measures adopted to avoid

individual responsibility for the compromise of protected information. The Board can advise on how much security is reasonable in terms of the sensitivity of particular data bases with respect to privacy considerations.

Adjudication of Disputes

Another of the Board's critical functions is to expedite the disposition of disputes; cut time, cost, and inconvenience to data subjects and executive departments alike; promote fairness and uniformity in information management protocols; and alleviate the burden on the federal court system resulting from protracted and expensive litigation involving the use and disclosure of government information. Accordingly, an office of administrative law judges should have the responsibility of resolving informational privacy disputes.

The adversary process of our federal judicial system has pursued a case-by-case resolution of privacy disputes without the guidance of a policy framework against which to measure competing interests. As a result, decisions are in conflict, and are not decided so as to present a consistent fabric of informational privacy policy. Administrative courts, tribunals within administrative agencies, may be a far superior alternative to the judicial branch:

> Unlike Article III judges, who can perform only adjudicative functions, agencies and legislative courts can apply their expertise not only to adjudication but also to rulemaking, administration, and reporting to Congress or other decisionmakers. Mixing adjudicative with administrative and rulemaking functions helps to adapt adjudication to the implementation of regulatory policies in a way that might not be possible within a scheme of rigidly separated powers.[34]

The Board should be empowered to resolve disagreements between agencies concerning interagency access to personal information; or disputes involving data subjects, agencies, and third parties with respect to the disclosure of personal information in light

of privacy interests and government information policy. An experienced administrative tribunal can simplify the process and provide consistency in the application of statutory policy.

In addition to deciding disputes, the administrative judges should be authorized to award damages and assess costs and attorney fees, as deemed appropriate. In case of appeal to an Article III court, review of administrative determinations is a far less expensive and complex process than entertaining the matter in the court *de novo*.

Organizational Structure

Desirable qualities reflected in the Board's membership and structure include these:

1. It should be nonpartisan because privacy is really a politically neutral interest. The Privacy Act, for instance, was cosponsored by Senator Edward Kennedy and Congressman Barry Goldwater, Jr., often political opposites.

2. The Board membership should be large enough to encompass a suitable scope of professional experience but not so large as to be unwieldy in consultation or deliberation. This determination is arbitrary within limits; a membership of three is probably too small, and nine is too large.

3. In addition to sitting collectively for rulemaking, or individually or in panels for hearings, the board members should be in active management of the Board's operating divisions. Day-to-day involvement in the processes of federal information management should enhance the members' experiential basis for policy analysis and guidance, and promote their intimate knowledge and control of Board functions and activities. Such a structure diminishes the likelihood that the members will be insulated from contact with agencies and users by a tier of top-level bureaucrats.

4. Tenure of members should be staggered and of sufficient duration to provide continuity, but not so lengthy as to inhibit the infusion of

fresh perspectives sensitive to new information technology and environment. This, too, is a rather arbitrary determination, though three years is too short a term and seven years is probably too long.

With these characteristics in mind, as well as the program elements and legal constraints previously discussed, here is a general prescription:

The Board should consist of a chairman and four other members appointed by the President and confirmed by the Senate, who should serve full-time. Not more than three members should be of the same political party, and none should serve contemporaneously as an officer, employee, or advisor of any other entity of federal government or the private sector. Members should be appointed for a term of five years, except that for initial appointments the Chairman and one member should be appointed for five years, and one member each for terms of two, three, and four years; no member should serve consecutive terms on the Board.

The Board, by majority vote, shall issue rules, regulations, advisory opinions, and directives, pursuant to the policies established in the authorizing legislation. The Board shall have power to authorize public hearings and to issue administrative subpoenas. The Board shall report annually to the President and to the Congress summarizing its findings and actions, and shall report promptly to the President and Congress regarding the failure of any agency to substantially comply with Board directives.

The Chairman will serve as chief executive officer and head the Board's administrative office. A member of the Board should head each of the following operational offices: administrative law judges, research and evaluation, auditing and enforcement, and general counsel.

The Board's administrative law procedures shall conform to the Administrative Practices Act, and decisions of the Board's administrative law judges shall be appealable to the Federal District

Court for the District of Columbia, or to other appropriate district court jurisdictions.

SOME FOREIGN MODELS

Several nations have enacted data protection laws which establish commissioners and registrars to oversee the implementation of privacy protection in government personal information systems. These nations include Canada, Federal Republic of Germany, France, Sweden, and the United Kingdom. It is interesting to note that though the United States was the first developed nation to entertain notions of informational privacy, other countries have moved ahead with more effective measures for data protection than have we. For purposes of comparison regarding the range of options adopted by others and those suggested in this paper, here follows a brief description of some foreign models.

The Swedish Data Act of 1973 created a Data Inspection Board to regulate all automated personal information systems in both the public and private sector. The Board exercises great power by inspecting and licensing systems; investigating complaints; and regulating, through its rule-making powers, the collection, use, and disclosure of information. The Swedish Act guarantees an individual the right to access and challenge information about himself, pursuant to the Board's rules.

The Federal Republic of Germany's Data Protection Act[35] also requires registration of both public and private sector automated information systems. The regulatory schemes, however, for private and government entities differ. Private sector information systems are regulated by state authorities. A Federal Commissioner of Data Protection, appointed for a five year term, oversees agency compliance with the Data Protection Act. The Commissioner investigates complaints, audits information systems, and recommends action. Though the Commissioner does not have any enforcement powers, he reports and makes recommendations to the Minister of the Interior and Parliament.

Canada's Privacy Act regulates information kept by certain governmental institutions listed on a Schedule attached to the act and periodically revised. The Act establishes a Privacy Commissioner appointed for a seven year term and accountable to Parliament. The Privacy Commissioner hears complaints from individuals regarding disclosure of personal information and denied requests to correct or annotate information kept in a file. The Commissioner also has broad investigatory powers to audit government compliance with the Privacy Act, and to compel testimony and production of evidence. The Commissioner makes recommendations in annual reports to Parliament, and may chastise government institutions that are failing to comply with the Act.

CONCLUSION

As a nation that prides itself on its respect for human dignity and individual rights, and that has been in the vanguard of recognizing informational privacy as an aspect of those values, it is ironic that we have fallen behind in adequately protecting that interest. The longer we wait, the more difficult it becomes to "retrofit" information technology so that protocols can provide appropriate protection. Rather than muse over whether we can protect privacy in this information society, we should set upon that task at the earliest possible time. The next important step is to establish a regulatory mechanism with the authority and resources to do the job. That, simply, is the proposal put forth.

Notes

1. A. Miller, *The Assault on Privacy* (1971).

2. A. Westin and M. Baker, *Data Banks in Free Society* (1972).

3. Secretary Advisory Comm. on Automated Personal Data Systems, U.S. Dept. of Health, Education and Welfare, *Records, Computers and the Rights of Citizens*, (1973) (OSHEW Publication No. (D)73-94).

> These principles have become the conventional wisdom of privacy advocates, and can be summarized as follows:
> 1. Maintain no secret personal information systems....
> 2. Collect only that personal information which has been authorized for a legal purpose....
> 3. Be sure that information is accurate, timely, and complete....
> 4. Give the data subject access and review rights to information about himself....
> 5. Use data only for the purpose for which it was collected....
> 6. Protect data against unauthorized use, loss, alteration, or disclosure.

Trubow, *Information Law Overview*, 18 J. Marshall L. Rev. 815, 822-23 (1985).

4. Pub. L. No. 93-579, 88 Stat. 1897, codified in part at 5 U.S.C. § 552a.

5. 28 C.F.R. §§ 20-1 *et seq.* (1987) (as amended) (originally published at 41 Fed. Reg. 11, 715 (March 19, 1976).

6. Privacy Protection Study Commission, *Personal Privacy in an Information Society* (1977).

7. American Bar Association, *Report on the National Symposium on Personal Privacy and Information Technology* and *Invited Papers on Privacy: Law, Ethics, and Technology* (1982).

8. Albinger, *Personal Information in Government Agency Records: Toward an Informational Right to Privacy*, 1986 Annual Survey of American Law 625 (cite omitted).

9. Mr. William Bailey, president of Aetna Life Insurance Co., was a member of the PPSC, and no doubt was instrumental in persuading his colleagues to implement responsible privacy standards.

10. The notion of "privacy" as a legal concept did not reach the United States from England because privacy was not recognized in the common law. Rather, Warren and Brandeis introduced the idea into American jurisprudence in their famous 1890 law review article. [Warren & Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).] The primary concern of those gentlemen was that private information had become increasingly public.

Trubow, *Information Law Overview*, 18 J. Marshall L. Rev. 815, 816-17 (1985).

11. For a discussion of the privacy torts, see, Trubow, *Tort Law of Privacy*, in 1 Privacy Law and Practice 1.01 (G. Trubow ed. 1987); W.P. Keeton, D. Dobbs, R. Keeton & D. Owen, *Prosser and Keeton on the Law of Torts* § 117 (5th ed. 1984).

12. For a discussion of constitutional privacy, see, L. Tribe, *American Constitutional Law* § 15-1 *et seq.* (2d ed. 1988).

13. The author does not claim to have created this phrase, though he believes he was present at the creation. The staff of the Executive Office of the President, Committee on the Right to Privacy, while wrestling with terminology in early 1974, adopted this usage. We think it is descriptively accurate and grammatically correct.

14. "Thus even the prevailing law of invasion of privacy generally

recognizes that the interests in privacy fade when the information involved already appears on the public record." *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469, 494-95, 95 S. Ct. 1029, 1046 (1975).

15. U.S. Congress, Office of Technology Assessment, *Computer-Based National Information Systems* 128 OTA-CIT-146 (September 1981). This cost analysis preceded the personal computer explosion of the early 1980s.

The evolving personal computer technology over the past two years, including the development of the 386 and forthcoming 486 chips, forthcoming CD-Rom technology, multi-tasking abilities, networking, communications, and relational data-bases, allows the small computer user inexpensive access to information around the world.

16. "Modern developments in information assembly drastically alter the access of third parties to personal information, decrease the costs of obtaining information, and increase the costs of secrecy." Dreyfuss and Leebron, *Forward: Privacy and Information Technology*, 1986 Annual Survey of American Law 495, 502.

17. "As of December 31, 1976, 97 agencies had filed notices on 6,753 systems containing 3.85 billion records." U.S. Privacy Protection Study Commission, *Appendix 4: The Privacy Act of 1974: An Assessment 11* (1977) *citing Federal Personal Data Systems Subject to the Privacy Act of 1974, Second Annual Report of the President, Calendar Year 1976*, 23. Of the notices filed in 1976, the Department of Defense had filed 32%; the Department of Treasury, 14%; and the Department of Health, Education, and Welfare, 12%.

"In 1983, federal agencies reported maintaining about 4,700 systems of records that have been estimated to contain personal information on virtually everyone in the country." General Accounting Office, *Privacy Act: Federal Agencies' Implementation Can Be Improved* 8 GAO/GGD-86-107 (Washington DC: General Accounting Office, August 1986).

As of December 31, 1985, federal agencies reported over 3,700 civilian record systems in effect. General Accounting Office, *Privacy Act System Notices*, Appendix I, 5 GAO/GGD-88-15BR (Washington DC: General Accounting Office, November 1987). (Having reviewed the notices on 53 randomly selected civilian records systems, the GAO concluded that 29 (55%) needed to be updated to reflect current conditions.)

In a study performed by the Office of Technology Assessment, 12 cabinet departments and 13 independent agencies reported on only

their 10 largest Privacy Act systems. The study showed that 3,458,900,000 records were stored in 539 systems of records. Of these records, 2,454,300,000 (71%) were in fully computerized systems. Another 303,600,000 (9%) records were in partially computerized systems. U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy* 23 OTA-CIT-296 (Washington DC: U.S. Government Printing Office, June 1986).

18. The OTA study of computerized and manual Privacy Act Record Systems maintained by 12 cabinet departments and 13 independent agencies showed that records on 1,664,851,377 persons were kept in fully computerized systems. Records on 290,006,794 persons were in partially computerized systems and on 700,762,623 persons in fully manual systems. By classifying the systems as large (over 500,000 persons), medium (10,001-500,000 persons), and small (under 10,000 persons), it becomes evident that the larger the system of records, the more likely that it is computerized. U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy* 23 OTA-CIT-296 (Washington DC: U.S. Government Printing Office, June 1986). The statistical tables do not, however, reveal whether a system is larger because it is fully computerized or *vice versa*.

19. "It seems that there should come a point when, in tenaciously tracking and piecing together the details of a person's life from multifarious sources, the resulting probe becomes so intrusive as to amount to an invasion of privacy even if the individual pieces of the probe are from public sources." *Alliance to End Repression* v. *City of Chicago*, 627 F. Supp. 1044, 1054 (N.D. Ill. 1985).

20. U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy* 108 OTA-CIT-296 (Washington DC: U.S. Government Printing Office, June 1986).

21. Tax Reform Act of 1986 §1524, I.R.C. §§ 6109 and 6676.

22. Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503 (1988) (to amend Privacy Act of 1974, 5 U.S.C. §552a).

23. The necessity to obtain personal information to administer the various federal benefits programs and the ability, through sophisticated computer technology, to store, collate and manipulate enormous amounts of information provided an impetus for federal privacy legislation. Data collection abuses that accompanied the surveillance of citizens by military, intelligence and law enforcement agencies and the Watergate scandal also spurred the enactment of the Privacy Act.

R. Ehlke, "The Privacy Act of 1974," 2.01[1] at 2-3 in *Privacy Law and Practice* (G. Trubow, ed., 1987).

24. Congress' Findings and Statement of Purpose were contained in Section 2 of Pub. L. 93-579:

(a) The Congress finds that

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use or dissemination or personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to

regulate the collection, maintenance, use, and dissemination of information by such agencies.

(b) The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to —

(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

(3) permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;

(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

(6) be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under this Act.

25. 5 U.S.C. § 552 (Supp. IV 1987).

26. Pub. L. 89-555, 80 Stat. 383 (1966), codified as amended at 5 U.S.C. § 552 (1982 and Supp. IV 1986).

27. While the Privacy Act was designed to provide *individuals* with more control over the gathering, dissemination, and accuracy of agency information about themselves, FOIA was intended to increase the *public's* access to governmental information.... It is readily apparent... that the Privacy Act and FOIA substantially overlap. However, it is apparent also that the two statutes are not completely coextensive; each provides or limits access to material not opened or closed by the other. For example, while both restrict access to investigatory material, they do so to a different degree and under different conditions.

Greentree v. *U.S. Customs Service*, 674 F.2d 74, 76 and 78 (D.C. Cir. 1982). In *Greentree* the court held that the Privacy Act is not an exempting statute within the meaning of Exemption 3 of FOIA which bars access under FOIA to information "specifically exempted from disclosure by" any other statute. *Contra.*, *Terkel* v. *Kelly*, 599 F.2d 214 (7th Cir. 1979) *cert. denied*, 444 U.S. 1013, 100 S.Ct. 662, 62 L.Ed.2d 642 (1980) (Privacy Act exemption from access to investigatory material compiled for law enforcement purposes applied to FOIA.); *Painter* v. *Federal Bureau of Investigation*, 615 F.2d 689 (5th Cir. 1980) (following *Terkel*).

Congress resolved this particular conflict by amending subsection (q) of the Privacy Act to provide that FOIA exemptions do not apply to the Privacy Act, and Privacy Act exemptions do not apply to FOIA. Pub. L. 98-477, § 2 (c), 98 Stat. 2211 (1984), as codified at 5 U.S.C. § 552a(q) (Supp. IV 1986). See also, Susman, *The Privacy Act and the Freedom of Information Act: Conflict and Resolution*, 21 J. Marshall L. Rev. 703 (1988).

However, one of the exemptions in FOIA is for "clearly unwarranted invasion of privacy," but the two acts do not interrelate and different standards apply to defining "privacy" under FOIA than under the Privacy Act.

28. U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and*

Individual Privacy 17 OTA-CIT-296 (Washington DC: U.S. Government Printing Office, June 1986).

29. U.S. General Accounting Office, *Privacy Act: Federal Agencies' Implementation Can Be Improved*, 47 GAO/GGD-86-107 (Washington DC: General Accounting Office, August 1986).

30. *FOIA: Alternate Dispute Resolution Proposals: Hearings Before the Subcomm. on Government Information, Justice, and Agriculture of the House Comm. on Government Operations*, 100th Cong., 1st Sess. 99 (1987) (statement of Francis J. Chetwynd, Partner, Cole, Raywid & Braverman).

31. American Bar Association, *Report on the National Symposium on Personal Privacy and Information Technology* and *Invited Papers on Privacy: Law, Ethics, and Technology* 8-9 (1982).

32. Some of the proposed bills were S. 786, "Information Age Commission Act of 1985", 99th Cong., 1st Sess.; H.R. 744 "Information Science and Technology Act of 1985", 99th Cong., 1st Sess.; and H.R. 1721, "Data Protection Act of 1985", 99th Cong., 1st Sess. See, U.S. Congress, Office of Technology Assessment, *Federal Government Information Technology: Electronic Record Systems and Individual Privacy* 119 OTA-CIT-296 (Washington, DC: U.S. Government Printing Office, June 1986).

33. Albinger, *Personal Information in Government Agency Records: Toward an Informational Right to Privacy*, 1986 Annual Survey of American Law 625, 642-43 (cites omitted).

34. Fallon, *Of Legislative Courts, Administrative Agencies, and Article III*, 101 Harv. L. Rev. 915, 935 (1988).

35. Bundesdatenshutzgesetz [BDSG] 1977 BGB1 I 202.

About This Series

This publication is one of eight papers that comprise the Benton Foundation Project on Communications & Information Policy Options. Papers may be ordered individually, or as a boxed set, by contacting the foundation at the address below.

Papers in this series include:

1 *The Role of Public Policy in the New Television Marketplace*
Jay G. Blumler
University of Leeds and University of Maryland

2 *Public Broadcasting*
Harry M. Shooshan III and Louise Arnheim
Shooshan & Jackson Inc.

3 *Charging for Spectrum Use*
Henry Geller and Donna Lampert
Washington Center for Public Policy Research
Duke University

4 *A Federal Right of Information Privacy: The Need for Reform*
Jerry Berman and Janlori Goldman
American Civil Liberties Union

5 *Watching the Watchers: The Coordination of Federal Privacy Policy*
George Trubow
The John Marshall Law School

6 *Strengthening Federal Information Policy: Opportunities and Realities at OMB*
Gary Bass and David Plocher
OMB Watch

7 *A Presidential Initiative on Information Policy*
John Shattuck and Muriel Morisey Spence
Harvard University

8 *The Federal Structure for Telecommunications Policy*
Henry Geller
Washington Center for Public Policy Research
Duke University

Individual copies are $6.50 each, including postage and handling. The boxed set of eight papers is available for $33.00, including postage and handling. A bulk discount of 10% is available for orders of 10 or more copies of the same paper. Checks or money orders should be made payable to the Benton Foundation and mailed to:

Policy Options Project
Benton Foundation
1776 K Street, N.W.
Washington, D.C. 20006

BENTON FOUNDATION

1776 K Street, N.W.
Washington, D.C. 20006